REMARKS

Claims 1-3, 10-12 and 19-48 are pending in the present application. Claims 1-3, and 10-12 are independent claims. None of the claims were amended in this response.

Claims 1-3, 10-12, and 19-48 were rejected under 35 U.S.C. §103(a) as being unpatentable over the publication "Data Communications, Computer Networks and Open Systems" by Halsall (herein after "*Halsall*") in view of Frezza (US Patent 4,982,430). Applicants respectfully traverse this rejection. Favorable reconsideration is earnestly requested.

Specifically, the cited art, alone or in combination, does not teach "a commutative operation which forms said first commutative checksum by operating on said segment checksums, and a cryptographic operation which cryptographically protects said first commutative checksum." As recited in claim 10, and similarly recited in claims 1-3 and 11-12. Applicants respectfully submit that the Halsall article does not teach or suggest a single method which combines the formation of a checksum with respect to data segments with a commutative linking of the checksums and, in a further combination, with a cryptographic encoding of the commutatively linked checksums.

Through the claimed commutative linking of segment checksums, a data stream may be checked independently of a sequence of the data packets in the data stream. Furthermore, through commutative linking, data segments need not arrive in the same order they were sent in order to compute a cryptographic operation on the checksum. Thus, regardless of the sequence of the data packets, a commutative linking of the individual segment checksums with respect to a commutative checksum independently of their linking sequence provides the same checkable value to be compared; i.e., the commutative checksum. It is therefore guaranteed by the forming of the checksum and by its subsequent commutative linking that the commutative checksum always receives the same value regardless of the sequence of the data segments. Furthermore, the present claims provide a cryptographic securing of the linking result. This further increases the security of the inventive method whereby the checksum is protected against manipulations.

With respect to independent claim 10, the Office Action asserted that *Halsall* teaches all of the elements of the claim expect for the feature "cryptographic operation which cryptographically protects said first commutative checksum." The Office Action also implies that *Halsall* nonetheless teaches that data encryption operations are standard implementation on

transmissions that require privacy on an unprotected network and are disclosed on page 719; 2nd paragraph of *Halsall*. To this end, the Office Action relies on Frezza in an attempt to cure the deficiencies of Halsall. However, Applicants respectfully submit that there is no teaching, suggestion or motivation for one skilled in the art to combine the references in the manner suggested in the Office Action.

The Office Action argues that error correction protocols and data encryption protocols are distinctly layered and thus require no additional modification for respective protocols to be implemented together on a network. However, if checksum computing and encryption were taking place in different layers, then the entire data stream would require encryption. The present claims recite that only the first commutative checksum is encrypted. While Halsall discloses a specific data encryption operation, Frezza encrypts the entire data stream of a CATV transmission, and also does not teach commutative linking. Also, while Frezza is directed to preventing pirated cable services, Halsall teaches checksum operations in the context of data error textual correction (3.4.1-3.4.2). One of ordinary skill in the art would find no motivation, either in the teachings of *Halsall*, Frezza, or in the knowledge known in the art, to utilize a method for encoding text with a commutative checksum, when the commutative checksum already achieves this objective. Thus, the combination is redundant and fails to apply the correct knowledge of ones ordinary skill in the art.

Furthermore, the first methodology taught by *Halsall* concerning finding a commutative checksum, does not teach encoding the sum and the second methodology concerning encoding does not teach a commutative checksum. As argued above, this is logically the case because to incorporate both methodologies into one, singular system would be redundant and, more importantly, nonsensical to one of ordinary skill in the art. Accordingly, the Applicants respectfully submit that *Halsall* does not teach or suggest all of the features of claimed 10, especially in view of the knowledge of one of ordinary skill in the art. Accordingly, the rejection of claim 10 should be withdrawn.

With respect to independent claims 1-3, 11 and 12, these claims are allowable for at least the same reason presented above with respect to independent claim 10. Moreover, dependent claims 19-48 are allowable on their merits and at least due to their respective dependencies on the independent claims, discussed above.

In light of the above, Applicants respectfully submit that independent claims 1-3 and 10-12 of the present application, as well as claims 19-48 which respectively depend therefrom, are both novel and non-obvious over the art of record. Accordingly, Applicants respectfully request that a timely Notice of Allowance be issued in this case. If any additional fees are due in connection with this application as a whole, the Examiner is authorized to deduct said fees from Deposit Account No.: 02-1818. If such a deduction is made, please indicate the attorney docket number (0112740-466) on the account statement.

Respectfully submitted,

BELL, BOYD & LLOYD LLC

BY _____

Peter Zura
Reg. No. 48,196
P.O. Box 1135
Chicago, Illinois 60690-1135
Phone: (312) 807-4208

Dated: May 2, 2005